Ajuste Direto 62/21/DCP/GACD/Auditoria de certificados qualificados à Chave Móvel Digital

Caderno de Encargos

cláusulas jurídicas ____ **3**

Cláusula 1.ª Objeto ____ *3*

Cláusula 2.ª Local da prestação de serviços ____ *3*

Cláusula 3.ª Duração ____ *3*

Cláusula 4.ª Preço base ____ *3*

Cláusula 5.ª Condições de pagamento ____ *3*

Cláusula 6.ª Propriedade intelectual ____ *4*

Cláusula 7.ª Sigilo ____ *5*

Cláusula 8.ª Proteção de dados ____ *5*

Cláusula 9.ª Cessão da posição contratual e subcontratação ____ *7*

Cláusula 10.ª Comunicações e notificações ____ *7*

Cláusula 11.ª Penalidades contratuais ____ *7*

Cláusula 12.ª Foro competente ____ *8*

Cláusula 13.ª Legislação aplicável ____ *8*

Cláusulas Técnicas ____ **8**

Cláusula 14.ª Descrição técnica do contrato ____ *8*

Cláusula 15ª Requisitos da equipa e Entidade a afetar aos serviços ____ *21*

Cláusula 16ª Planeamento ____ *21*

Cláusula 17ª Entregáveis e documentação ____ *21*

Cláusula 18ª Mecanismos formais de acompanhamento ____ *22*

Cláusula 19ª Gestor do Contrato ____ *22*

CLÁUSULAS JURÍDICAS

Cláusula 1.ª

Objeto

O presente caderno de encargos compreende as cláusulas a incluir no contrato a celebrar com a Agência para a Modernização Administrativa, IP, (doravante abreviadamente designada por "AMA"), na sequência de procedimento pré-contratual que tem por objeto a prestação de serviços de auditoria de acompanhamento a Serviços de confiança de certificados qualificados de assinaturas eletrónica, com serviço de aposição de assinatura eletrónica qualificada criada através de dispositivo de criação das assinaturas eletrónicas à distância, do Prestador Qualificado de Serviços de Confiança AMA, nos termos melhor definidos nas cláusulas técnicas do presente caderno de encargos.

Cláusula 2.ª

Local da prestação de serviços

O local da prestação de serviços será nas instalações da AMA, no Datacenter onde estão alojadas as soluções (na área metropolitana de Lisboa), e nos locais de registo na Chave Móvel Digital em território nacional nas instalações do cocontratante.

Cláusula 3.ª

Duração

O contrato terá a duração de 4 semanas contados da data da sua celebração, sem prejuízo das obrigações acessórias que devam perdurar para além da sua cessação.

Cláusula 4.ª

Preço base

1. O preço base é de € 19.000,00 (dezanove mil euros) a que acresce o IVA à taxa legal em vigor.
2. São excluídas as propostas cujo valor seja superior ao preço base.
3. O preço referido no n.º 1 inclui todos os custos, encargos e despesas cuja responsabilidade não esteja expressamente atribuída à AMA, designadamente
    a) Despesas com deslocações, estadias e despesas de alimentação;
    b) Encargos com telecomunicações;
    c) Seguro de acidentes de trabalho.

Cláusula 5.ª

Condições de pagamento

1. A faturação é efetuada nos seguintes termos:
    a) 60% do preço contratual com a entrega Relatório de Auditoria de à CMD, previsto na alínea a) do n.º 1 da cláusula 17.ª do presente caderno de encargos;
    b) 20% do preço contratual com a aceitação do Relatório de Auditoria à CMD;
    c) 20% do preço contratual com a entrega e aceitação de todos os serviços objeto do presente procedimento;
2. O pagamento será efetuado no prazo 30 dias a contar da data da receção das faturas correspondentes, as quais só podem ser emitidas após o vencimento da obrigação a que se referem.
3. As faturas devem discriminar os serviços a que se reportam, o número do contrato bem como o número de compromisso financeiro associado, o qual será indicado pela AMA, sob pena da sua devolução.
4. Caso as faturas apresentadas não sejam validadas pela AMA esta comunicará tal decisão ao cocontratante para que proceda à sua substituição.
5. As faturas poderão revestir a forma eletrónica, caso em que deverão ser remetidos à AMA através de meio de transmissão escrita e eletrónica de dados para o endereço fornecedores@ama.pt.
6. Só serão devidos os valores referentes às tarefas efetivamente prestadas e aceites nos termos do presente caderno de encargos.
7. O pagamento será realizado para o NIB/IBAN indicado em documento bancário apresentado pelo cocontratante o qual deverá ser atualizado sempre que necessário.
8. Em caso de atraso no cumprimento das obrigações pecuniárias por parte da AMA, o cocontratante tem o direito aos juros de mora sobre o montante em dívida, nos termos previstos no artigo 326.º do CCP e da Lei n.º 3/2010, de 27 de abril.

Cláusula 6.ª

Propriedade intelectual

1. São da responsabilidade do cocontratante quaisquer encargos decorrentes da utilização, na prestação de serviços, de marcas registadas, patentes registadas ou licenças.
2. O cocontratante obriga-se a transferir a posse e a propriedade dos elementos a desenvolver ao abrigo do contrato para a AMA incluindo os direitos autorais sobre todas as criações intelectuais abrangidas pelos serviços a prestar, incluindo os previstos no n.º 4 do artigo 14.º e 49.º, ambos do Código do Direito de Autor e dos Direitos Conexos, bem como de outros direitos de propriedade intelectual, relativos aos serviços objeto do presente caderno de encargos, produtos dele resultantes nomeadamente, documentação e elementos afins, bem como dos produtos consequentes a todas as ulteriores adaptações que se venham a revelar necessárias.
3. O cocontratante entregará à AMA no termo do contrato toda a documentação e desenvolvimento, relativo aos trabalhos desenvolvidos, incluindo as respetivas fontes que serão propriedade da AMA.

4. A AMA poderá reproduzir todos os documentos, bem como proceder à sua distribuição, onerosa ou gratuita, de forma inteiramente livre.
5. Pela cessão dos direitos a que alude o número anterior não é devida qualquer contrapartida para além do preço a pagar nos termos do presente caderno de encargos.

Cláusula 7.ª

Sigilo

1. O cocontratante obriga-se a observar sigilo quanto a informação e documentação, técnica e não técnica, comercial ou outra, relacionada com a atividade da AMA ou qualquer outra entidade envolvida na execução do contrato.
2. A informação e documentação cobertas pelo dever de sigilo não podem ser transmitidas a terceiros, nem ser objeto de qualquer uso ou modo de aproveitamento que não o destinado direta e exclusivamente à execução do contrato.
3. O cocontratante obriga-se ainda a respeitar a confidencialidade sobre todos os dados ou informações de carácter funcional ou processual dos serviços da Administração Pública a que tenha acesso na execução do contrato.
4. O cocontratante assume igualmente o compromisso de remover e destruir, no final do contrato, todo e qualquer registo, eletrónico ou em papel, relacionado com os dados e processos analisados e que a AMA lhe indique para esse efeito.
5. O cocontratante obriga-se, de um modo especial, a guardar sigilo quanto ao conteúdo e utilização dos sistemas de informação da responsabilidade da AMA, nos termos legalmente previstos, relativa à proteção de dados pessoais e a relativa à proteção jurídica de bases de dados.
6. Após ter conhecimento de alguma violação de dados pessoais o cocontratante notifica a AMA sem demora injustificada, em prazo inferior a 48 horas.
7. O cocontratante garante que terceiros que envolva na execução dos serviços respeitem as obrigações de sigilo e confidencialidade constantes nos números anteriores.

Cláusula 8.ª

Proteção de dados

1. O Cocontratante é obrigado a tratar todos os dados pessoais a que tiver acesso, de acordo com o previsto no Regulamento Geral de Proteção de Dados Pessoais aprovado pelo Regulamento (EU) 2016/679 do Parlamento Europeu e do Conselho de 27 de abril de 2016 (RGPD), devendo, nomeadamente:
    a) Tratar os dados pessoais apenas mediante instruções documentadas da Entidade Adjudicante, incluindo no que respeita às transferências de dados para países terceiros ou organizações internacionais, a menos que seja obrigado a fazê-lo pelo direito da União ou do Estado-Membro a

que está sujeito, informando nesse caso a Entidade Adjudicante desse requisito jurídico antes do tratamento, salvo se a lei proibir tal informação por motivos importantes de interesse público;

b) Assegurar que as pessoas autorizadas a tratar os dados pessoais assumiram um compromisso de confidencialidade ou estão sujeitas a adequadas obrigações legais de confidencialidade;

c) Adotar todas as medidas exigidas nos termos do artigo 32.º do RGPD;

d) Garantir o cumprimento do RGPD, nas condições aqui previstas, quando pretenda contratar um subcontratante;

e) Tomar em conta a natureza do tratamento, e na medida do possível, prestar assistência à Entidade Adjudicante pelo tratamento através de medidas técnicas e organizativas adequadas, para permitir que este cumpra a sua obrigação de dar resposta aos pedidos dos titulares dos dados tendo em vista o exercício dos direitos previstos no capítulo III do RGPD;

f) Prestar assistência à Entidade Adjudicante no sentido de assegurar o cumprimento das obrigações previstas nos artigos 32.º a 36.º do RGPD, tendo em conta a natureza do tratamento e a informação ao seu dispor;

g) Consoante a escolha da Entidade Adjudicante, apagar ou devolver-lhe todos os dados pessoais depois de concluído o contrato, apagando as cópias existentes, a menos que a conservação dos dados seja exigida ao abrigo do direito da União ou dos Estados-Membros;

h) Disponibilizar à Entidade Adjudicante todas as informações necessárias para demonstrar o cumprimento das obrigações previstas na presente cláusula, facilitando e contribuindo para as auditorias, inclusive as inspeções, conduzidas pela Entidade Adjudicante ou por outro auditor por esta mandatado.

2. A Entidade Adjudicante, no caso de suspeitar de incumprimento do RGPD, pode notificar o Cocontratante para este, no prazo de 5 dias, demonstrar o total cumprimento do referido regulamento.

3. Caso o Cocontratante não demonstre o total cumprimento do RGPD, seja porque não o demonstrou, seja porque não o cumpre, a Entidade Adjudicante fica autorizada a proceder à auditoria aos sistemas de informação do Cocontratante, ficando este responsável por todos os custos dessa auditoria.

4. No caso previsto no número anterior, a Entidade Adjudicante poderá compensar os custos que tenha suportado com eventuais quantias que sejam devidas ao Cocontratante, ou através do acionamento da caução, caso esta tenha sido prestada, ou através do recurso às retenções que eventualmente tenham sido efetuadas.

5. No caso de se verificar algum incumprimento do RGPD por parte do Cocontratante, este deverá, no prazo de 10 dias, por fim ao incumprimento e demonstrá-lo à Entidade Adjudicante.

6. O não cumprimento do RGPD, por facto imputável ao cocontratante, é considerado, para todos os efeitos, incumprimento definitivo, podendo a Entidade Adjudicante resolver o contrato, ao abrigo da alínea a) do n.º 1 do artigo 333.º do CCP.

7. Caso o Adjudicatário impeça ou não colabore na realização da auditoria referida no n.º 3 da presente cláusula, a Entidade Adjudicante poderá resolver o contrato, por oposição reiterada ao exercício dos poderes de fiscalização, ao abrigo da alínea c) do n.º 1 do artigo 333.º do CCP.

Cláusula 9.ª

Cessão da posição contratual e subcontratação

O cocontratante não pode ceder a sua posição no contrato ou subcontratar total ou parcialmente os serviços incluídos no mesmo.

Cláusula 10.ª

Comunicações e notificações

1. Sem prejuízo de se acordarem outras regras quanto às notificações e comunicações entre as partes, estas devem ser dirigidas para o domicílio ou sede contratual de cada uma nos termos previstos no contrato.
2. Qualquer alteração das informações de contacto constantes do contrato deve ser comunicada à outra parte.

Cláusula 11.ª

Penalidades contratuais

1. Pelo incumprimento de obrigações emergentes do contrato, a AMA pode exigir ao cocontratante o pagamento de uma sanção pecuniária, num montante a fixar em função da gravidade do incumprimento, nos seguintes termos:
    a) Pelo incumprimento nos prazos de apresentação dos entregáveis acordados, serão aplicadas penalidades de até 0,5% do preço contratual por cada dia de atraso;
2. Na determinação da gravidade do incumprimento, a AMA tem em conta, nomeadamente, a duração da infração, a sua eventual reiteração, o grau de culpa do cocontratante e as consequências do incumprimento.
3. A sanção aplicada será descontada na fatura imediatamente seguinte ao facto que a originou ou, caso tal não seja possível, será emitida nota de crédito.
4. O valor acumulado das sanções pecuniárias não pode exceder 20 % do preço contratual, sem prejuízo do poder de resolução do contrato.
5. Nos casos em que seja atingido o limite previsto no número anterior e a AMA decida não proceder à resolução do contrato, por dela resultar grave dano para o interesse público, aquele limite é elevado para 30 %.
6. A aplicação das sanções previstas na presente cláusula será objeto de audiência prévia, nos termos previstos no n.º 2 do artigo 308.º do Código dos Contratos Públicos.

Cláusula 12.ª

Foro competente

Para a resolução de todos os litígios relativos, designadamente, à interpretação, execução, incumprimento, invalidade, resolução ou redução do contrato é competente o Tribunal Administrativo de Círculo de Lisboa.

Cláusula 13.ª

Legislação aplicável

Em tudo o omisso neste Caderno de Encargos, observar-se-á o previsto no Código dos Contratos Públicos e demais legislação aplicável.

CLÁUSULAS TÉCNICAS

Cláusula 14.ª

Descrição técnica do contrato

1. Enquadramento

A AMA – Agência para a Modernização Administrativa, IP é a entidade responsável pela operacionalização de vários processos transversais que têm por objetivo melhorar a Administração Pública Portuguesa e disponibilizar serviços públicos pelo canal que o cidadão considere mais adequado.

A identificação inequívoca do cidadão perante os serviços públicos é uma necessidade premente à massificação na utilização dos serviços públicos na sua eletrónica, tendo a AMA vindo a desenvolver um conjunto de soluções de autenticação e de assinatura eletrónica qualificada com o Cartão de Cidadão (CC) de forma a garantir a toda a Administração Pública a possibilidade de integrar estas funcionalidades nos seus portais de forma simples e eficiente.

A Chave Móvel Digital (CMD) surgiu em 2015 como um meio simples e seguro de autenticação dos cidadãos em portais e sítios da Administração Pública na Internet, com dois fatores de segurança: uma palavra-chave e um código recebido por SMS. Tendo por base a importância da experiência de utilização, desde 2018 que é também possível a realização de assinaturas qualificadas com CMD "server-side".

Após a concessão da AMA enquanto serviço eletrónico de confiança para a criação de certificados qualificados de assinaturas eletrónicas, é necessário, nos termos dos normativos aplicáveis, proceder à aferição periódica de

procedimentos de segurança na infraestrutura da solução de assinatura do Fornecedor de Serviços de Confiança AMA (onde se destaca a chave móvel digital e o Serviço de Assinatura de Faturas Eletrónicas).

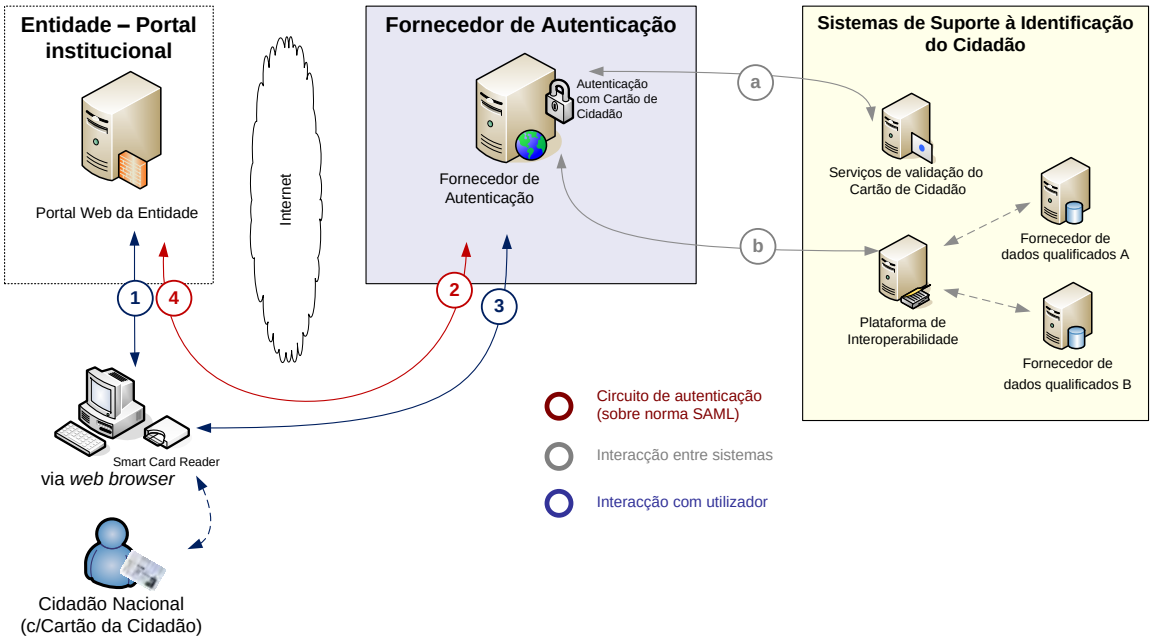
2. Plataformas Tecnológicas Relevantes para os Serviços a Prestar

Nesta secção apresenta-se uma descrição sucinta de projetos já realizados ou em curso que se consideram relevantes no âmbito deste procedimento.

2.1. Autenticação.Gov

O Autenticação.Gov (ou Fornecedor de Autenticação) surge na necessidade de identificação unívoca de um utilizador portador de um Cartão de Cidadão junto dos sítios Web de cada Organismo, com a obtenção da respetiva identificação setorial. Esta solução tem por objetivo tornar-se o ponto de autenticação eletrónica dos cidadãos perante a administração pública e mesmo organismos privados. O fornecedor de autenticação pretende assim facilitar e a acelerar o processo de adesão e utilização do cartão de cidadão na autenticação eletrónica do cidadão perante os serviços públicos.

A figura seguinte exemplifica a utilização do Autenticação.Gov com base num caso de uso de autenticação de um Cidadão junto de um Organismo.



No diagrama acima identificam-se as seguintes interações:

1. Cidadão pretende aceder à área privada do portal de um Organismo, ao qual é necessário que apresente a sua identidade;

2. Portal do Organismo delega a autenticação e redireciona o Cidadão para o Fornecedor de Autenticação, juntamente com um pedido de autenticação assinado digitalmente;

3. Cabe ao FA validar o pedido de autenticação recebido e solicitar a autenticação do Cidadão com Cartão de Cidadão, através da inserção do PIN. Durante este processo, o FA irá efetuar as seguintes operações internas:

    a) Validação das credenciais do Cidadão com recurso à PKI do Cartão de Cidadão, via OCSP;
    b) Obtenção de atributos que sejam solicitados através dos vários fornecedores de atributos qualificados, via Plataforma de Interoperabilidade. Este processo pode incluir a obtenção de dados da Federação de Identidades ou de outros Organismos;

4. A identidade e atributos do Cidadão são validados e assinados digitalmente pelo FA, que redirecionará o Cidadão de volta ao portal do Organismo original. Cabe ao Organismo a validação e utilização dos mesmos.

Dado que no processo de autenticação poderão ser solicitados mais dados que os presentes no certificado digital do Cartão de Cidadão (Nome e Número de Identificação Civil), mostra-se necessário a obtenção destes dados junto de fornecedores de atributos qualificados para o efeito.

2.2. Plataforma de Interoperabilidade da Administração Pública

A Plataforma de Interoperabilidade da Administração Pública fornece, entre outros aspetos, mecanismos robustos de autenticação e gestão de identidades, que facilitam a autenticação segura perante os organismos públicos, e mecanismos de controlo transacional, que garantem a qualidade dos dados durante o processo de utilização dos serviços eletrónicos, para além de um *gateway* central para os processos de pagamento eletrónico.

Na conceção do modelo da plataforma, os standards abertos impuseram-se sempre como opção estratégica, no sentido de assegurar um maior nível de interoperabilidade.

A adoção de uma Arquitetura Orientada a Serviços para a implementação de sistemas complexos e de grande dimensão, como é o caso de soluções de integração para a Administração Pública, assegura os níveis de adaptabilidade e rigor perante a mudança que é possível antecipar, deixando aberta a porta a evoluções e melhorias que se mostrem necessárias.

Esta tipificação arquitetural fornece um enquadramento sustentado, com um conjunto de regras e práticas que permitem a exposição de funções relevantes, enquanto serviços no nível de granularidade certo para quem deles

usufrui. Os serviços são expostos escondendo a mecânica de implementação e utilizando um formato de interface único e baseado em standards.

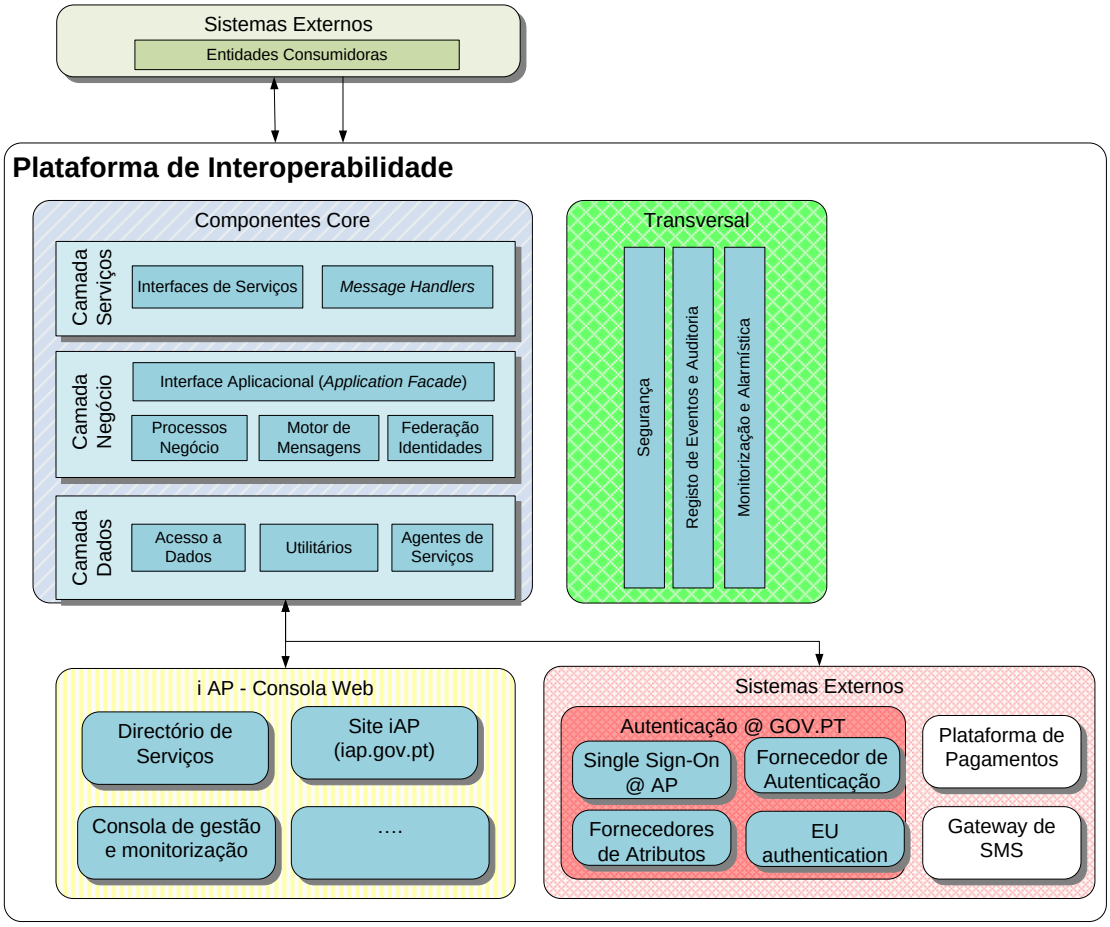


Figura 1 – Arquitetura lógica

A Plataforma de Interoperabilidade encontra-se suportada por um conjunto de componentes que visam atingir o objetivo para que a mesma foi criada. A sua arquitetura pode ser decomposta em várias áreas de atuação:

- **Componentes *core*** – agrega os componentes nucleares à utilização da plataforma como ferramenta de apoio à integração e serviço de dados. Encontram-se incluídas nesta área os componentes adaptadores aos diversos sistemas das Entidades, *pipelines* internos de processamento de mensagens, gestor de orquestrações e Federação de Identidades;
- **Componentes transversais** – abrangem todas as áreas da Plataforma de Interoperabilidade e são responsáveis pelas funcionalidades de segurança, privacidade de dados, registo e tratamento de exceções, bem como de monitorização global.

- **iAP – Consola Web** – apresentam-se como a camada visível da Interoperabilidade e partilha de serviços na Administração Pública. Providenciam uma imagem integrada da informação e funcionalidades disponíveis para as entidades públicas. Incluem-se neste domínio os componentes de:
  - **Diretório de Serviços** – responsável pela listagem e gestão dos serviços eletrónicos disponibilizados pela Plataforma;
  - **Consola de Gestão** – disponibiliza aos seus utilizadores (a Administração Pública), funcionalidades de gestão e monitorização da plataforma, específicas para as Entidades que representam. Permite acesso à gestão de serviços, bem como a monitorização e gestão operacional de serviços que se encontrem em utilização;
  - **Site i-AP** – ponto visível do exterior da plataforma, com informação referente aos serviços, funcionalidades, informação para utilização da plataforma, materializado através de sítio Internet www.iap.gov.pt.
- **Sistemas externos** – funcionam de forma independente, mas intimamente acoplados no domínio da Plataforma de Interoperabilidade. São subsistemas que possuem funcionalidades específicas, mas basilares ao funcionamento de toda a arquitetura, servindo como elementos de suporte e de valor acrescentado. Incluem-se neste domínio os componentes de:
  - **Autenticação @gov.pt** – conjunto de componentes que disponibilizam mecanismos de autenticação eletrónica perante a Administração Pública (e entidades privadas que o pretendam), assegurando funcionalidades de:
    - Fornecedor de Autenticação – descrito na secção seguinte;
    - Autenticação de Cidadãos da EU – possibilitando o acesso a serviços da Administração Pública Portuguesa por parte de cidadãos de outros Estados Membros e o acesso de cidadãos Portugueses a serviços eletrónicos de outros Estados Membros;
    - Fornecedor de Atributos – permite a obtenção de Atributos, tendo por base a autorização explícita do cidadão, para a execução de serviços eletrónicos, pelo canal Internet.
    - *Single-sign-on* – descrito na secção seguinte e nos serviços solicitados no âmbito deste procedimento.
  - **Plataforma de Pagamento e Gateway de SMS** – sistemas externos, já existentes e em utilização produtiva, que se pretende que sejam disponibilizados de forma integrada e sejam potenciados pela Plataforma de Interoperabilidade, especialmente com a utilização de serviços compostos ou em processos orquestrados inteiramente.

2.3. Chave Móvel Digital

A Chave Móvel Digital (CMD) é um meio simples e seguro de autenticação dos cidadãos em portais e sítios da Administração Pública na Internet, com dois fatores de segurança: uma palavra-chave e um código recebido por SMS. Com a CMD pode autenticar-se eletronicamente utilizando um computador ou dispositivos móveis com ligação à internet

As principais vantagens da CMD para o cidadão são:

- Mais simples: uma senha de acesso para todos os portais do Estado que disponibilizam este meio de autenticação.
- Mais seguro: inclui dois mecanismos de segurança: uma palavra-chave e um código temporário recebido por SMS no telemóvel registado.
- Mais cómodo: evita deslocações aos serviços públicos e tempos de espera.

Do ponto de vista funcional a utilização da CMD passa pelos seguintes passos:
1 – O cidadão acede ao portal ou sítio da Administração Pública na Internet
2 – O cidadão insere a sua identificação (número de telemóvel) e palavra-chave
3 – O cidadão recebe por SMS o código de utilização único por cada autenticação gerado pela CMD para confirmar os dados e concluir a autenticação
4 – O cidadão insere o código no computador
5 – O cidadão faz Login

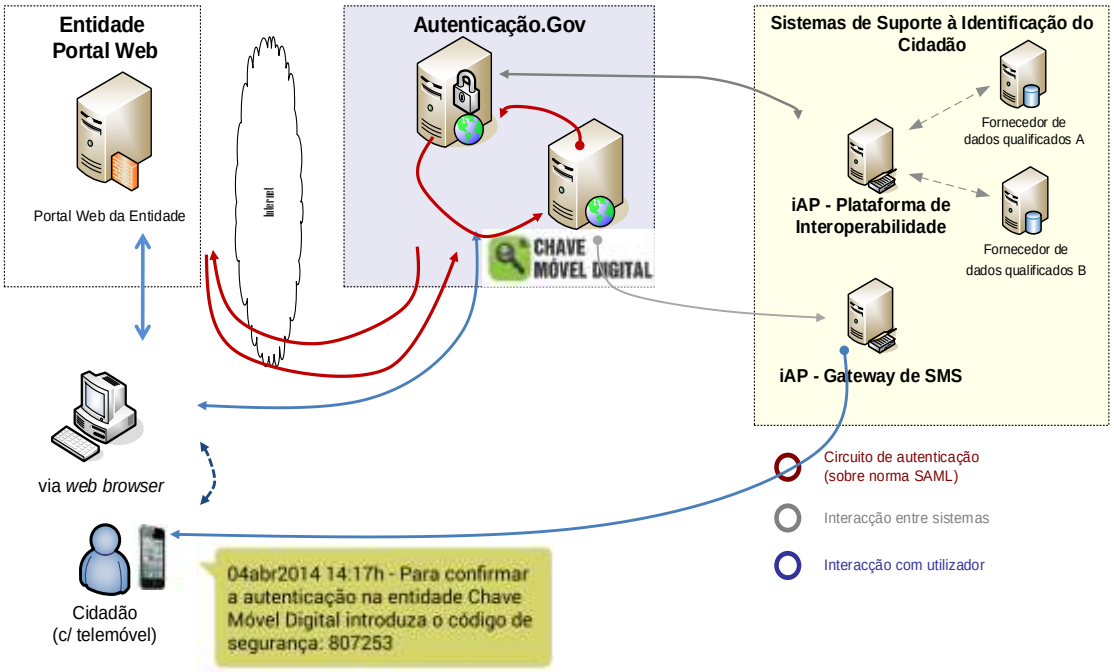
Para ativar, o cidadão deve dirigir-se a uma Loja do Cidadão, Balcão Multisserviços ou Espaço do Cidadão para obter a CMD e apresentar o seu Cartão de Cidadão ou Bilhete de Identidade. A ativação do serviço é gratuita.
É ainda possível fazer o registo online na CMD (sem deslocação presencial), fazendo uso do Cartão de Cidadão.

A CMD encontra-se já disponível em vários portais e sistemas (como Portal do Cidadão, Portal do Utente, entre outros), assegurando:

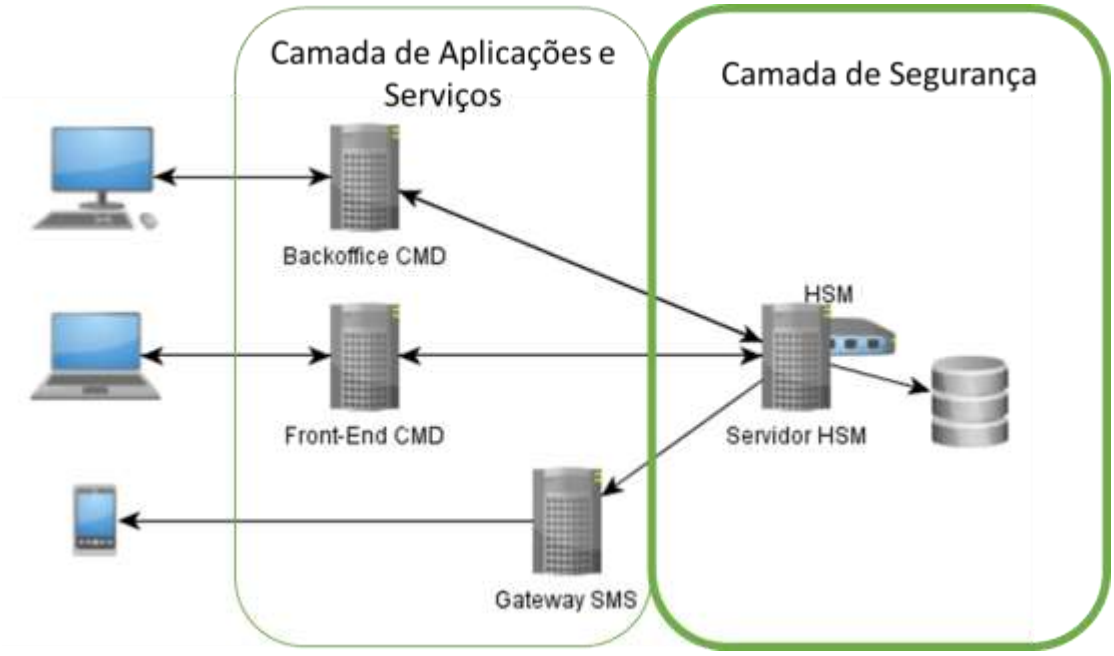
- Maior eficácia e elevada segurança: o registo é imediato, não obriga a processos de confirmação da identidade do cidadão como o envio de cartas para o domicílio de cidadão, nem a processos de reenvio de senhas, no caso de esquecimento da mesma.
- Fácil migração: caso o portal público já disponibilize autenticação com o Cartão de Cidadão utilizando o serviço Autenticação.Gov (vulgo Fornecedor de Autenticação) – como já acontece com os principais Portais que disponibilizam serviços públicos, como o Portal do Cidadão, o Portal da Empresa, o Portal

das Finanças, o Portal da Saúde, o Portal da Segurança Social, entre outros - para disponibilizar a autenticação com CMD num portal, basta incluir no atual pedido ao serviço "Autenticação.Gov" um parâmetro que indica que o portal também aceita Chave Móvel Digital.

A figura seguinte apresenta o fluxo global da solução implementada.



Encontra-se disponível mecanismo de assinatura associado à CMD, conforme arquitetura patente na figura seguinte:



O Secure Creation Device utilizado, para a aposição de assinatura eletrónica, é um HSM Thales nShield que já se encontra referenciado na compilação de informação dos estados membros sobre "Secure Signature Creation Devices benefiting from the transitional measure set in article 51(1) of Regulation 910/2014 (https://ec.europa.eu/futurium/en/system/files/ged/sscds-qscds_list_08052017.pdf)".

2.4. Serviço de Assinatura da Faturas Eletrónicas (SAFE)

O Decreto-Lei n.º 28/2019, de 15 de fevereiro torna obrigatória a emissão de faturas eletrónicas por intermédio do uso de uma assinatura digital qualificada ou de um selo eletrónico qualificado, a partir de Janeiro 2021.

Neste contexto, e também da medida do programa Simplex "Fatura eletrónica mais acessível", a AMA implementou o Serviço de Assinatura de Faturas Eletrónicas (SAFE), enquadrado no Sistema de Certificação de Atributos Profissionais (SCAP), com o objetivo de oferecer uma solução segura e simples de assinatura eletrónica qualificada de faturas à Economia.

Arquitetura da solução

O Serviço de Assinatura de Faturas Eletrónicas (SAFE) tem como objetivo de oferecer uma solução para a assinatura eletrónica qualificada em conformidade com o referido enquadramento legal. Este serviço público permite a administradores, gerentes, diretores ou outros por estes designados, sem custos adicionais, assinar faturas de forma simples e segura através de integração com os respetivos softwares de faturação.

O SAFE vem adicionar a funcionalidade de assinatura de faturas ao já existente SCAP - Sistema de Certificação de Atributos Profissionais (www.autenticacao.gov.pt).

Este serviço permite ao cidadão, enquanto profissional de uma empresa, assinar digitalmente faturas eletrónicas, através de mecanismo automatizado pelo software de faturação.

Assim, o empresário aderente ao SCAP (em moldes similares aos atuais), passa a ter acesso a novo certificado qualificado especifico para a assinatura de faturas. Este certificado tem uma duração máxima de 45 dias (de acordo com articulação com o GNS), podendo o empresário (registado no SCAP) proceder à sua emissão inicial e reemissão periódica (tipicamente mensalmente). Este processo é sumariado na figura seguinte.

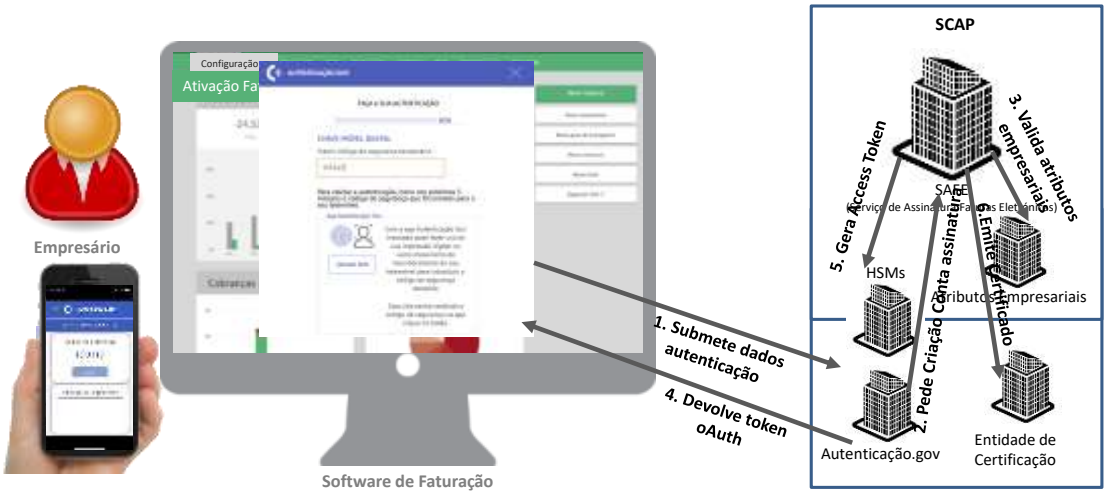


Figura 2 – Emissão periódica de certificado para emissão de fatura

Assim, de forma a obter um certificado de assinatura de faturas SAFE, o empresário/comerciante autentica-se com o Cartão de Cidadão ou a Chave Móvel Digital e, após verificação da existência de poder associado (no SCAP) para assinatura de faturas, é gerado um código ("Access Token") que é guardado de forma segura no software de faturação. Este "Access Token" permitirá a assinatura de faturas pelo empresário, sem necessitar de voltar a colocar qualquer PIN, durante um período até 45 dias (ou com o atingimento de um limite máximo de faturas).

No processo corrente, de emissão de faturas, a sua assinatura eletrónica é "transparente" para o empresário, conforme figura seguinte.

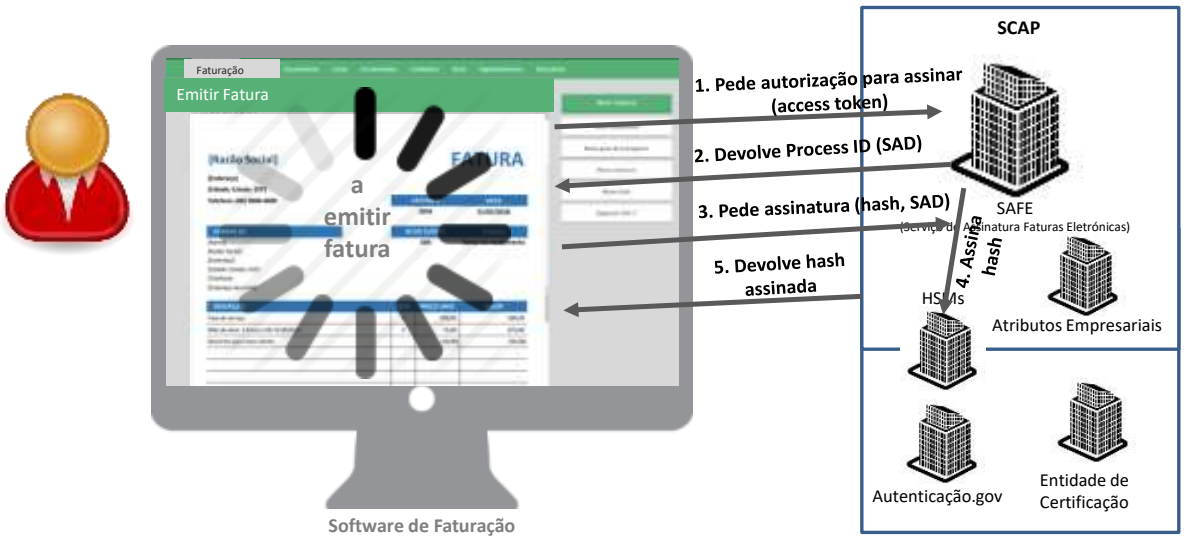


Figura 3 – Assinatura de fatura com SAFE

Assim, aquando da emissão da fatura, o software de faturação (devidamente autenticado) envia para o SAFE o "Acess token" (obtido aquando da ativação periódica do certificado, previamente descrito) e, seguindo uma sequência standard para a geração de assinaturas, é gerado um identificador do processo de assinatura que, quando enviado em conjunto com a hash da fatura, permite a sua assinatura pelo SAFE. Finalmente o software de faturação agrega a hash assinada da fatura, com o documento da fatura (que nunca é enviado para o SAFE), e disponibiliza a fatura assinada ao empresário.

Desta forma, o empresário/comerciante consegue assinar faturas eletrónicas, sem ter de adquirir qualquer hardware local adicional (e.g., leitor de smartcard) ou de realizar qualquer ação adicional (como a introdução de qualquer PIN), em cada assinatura.

A garantia de autenticidade da origem desta fatura, assim como à garantia de integridade da mesma, é utilizado o procedimento de aposição de assinatura eletrónica qualificada, em que a chave privada de assinatura é guardada centralmente de forma segura. O detentor da chave privada de assinatura (gerente/responsável da empresa com poderes para emitir e assinar faturas) terá de autorizar a utilização da mesma pelo software de faturação, sempre que a mesma é emitida ou renovada.

Descrição técnica mais detalhada

O Serviço de Assinatura de Faturas Eletrónicas (SAFE) está inserido no ecossistema Autenticacao.Gov (vide Figura 4), tirando proveito das funcionalidades de sistemas já existentes. Nomeadamente:

- Fornecedor de Autenticação (**FA**) – responsável pela autenticação de cidadãos, podendo os cidadãos utilizar a Chave Móvel Digital (CMD) ou o Cartão de Cidadão (CC) para proceder à sua autenticação. Após correta autenticação, o FA comunica com o SAFE para criação de conta de assinatura de faturas eletrónicas;
- Sistema de Certificação de Atributos Profissionais (**SCAP**) – responsável pela gestão e obtenção de atributos, em particular, os empresariais de cidadãos. O SAFE comunica com o SCAP para verificar se um cidadão tem o atributo necessário para criar uma conta de assinatura de faturas eletrónicas.

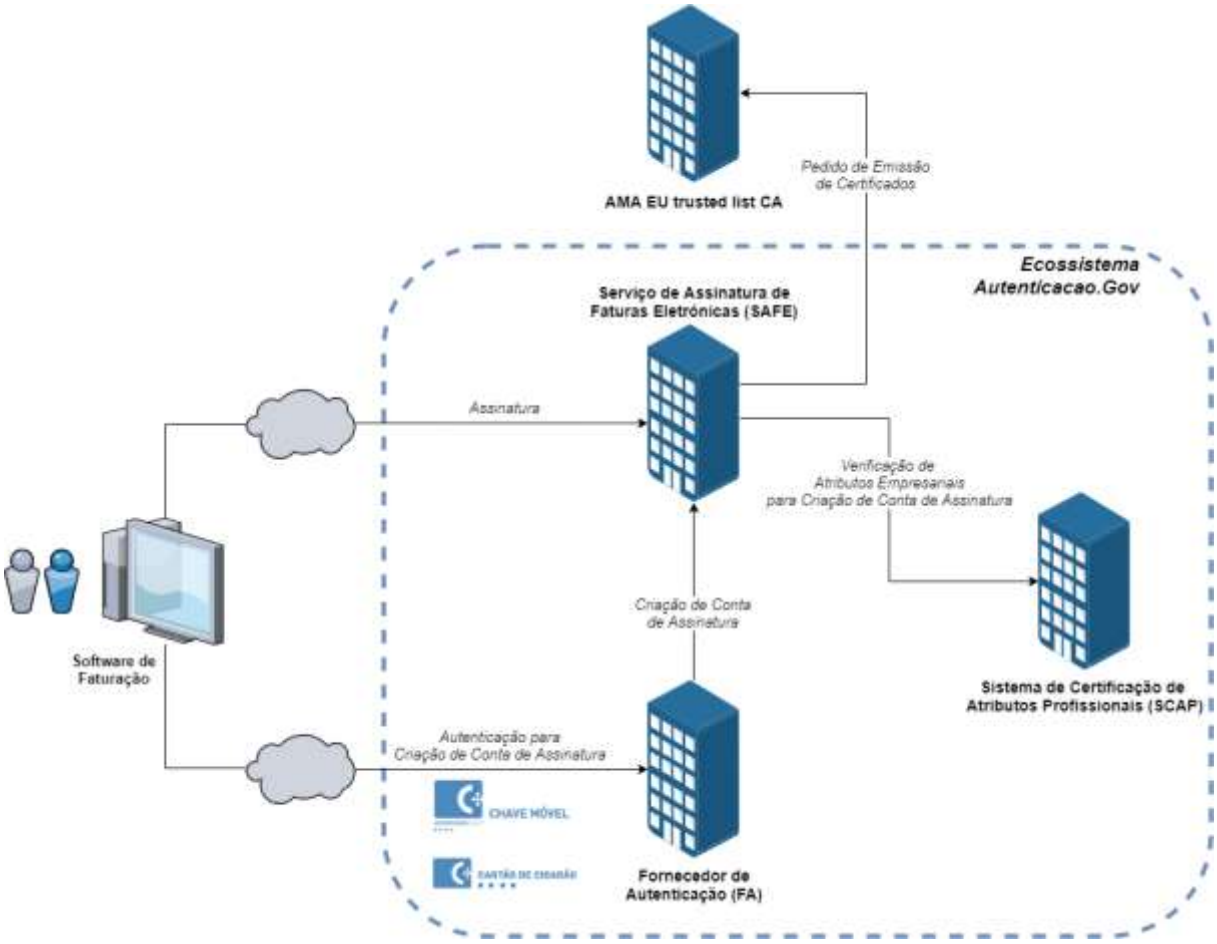


Figura 4 – Ecossistema Autenticação.gov

A Figura 5 ilustra um exemplo de um fluxo típico da comunicação entre o Software de Faturação, o serviço Autenticação.gov (FA) e o SAFE. O fluxo começa com o Software de Faturação a comunicar com o FA pedindo a criação de uma conta de assinatura.

Após a correta criação de conta, o Software de Faturação passa a comunicar exclusivamente com o SAFE, enviando o AccessToken ou o RefreshToken obtidos na criação de conta (certificado). Estes tokens devem ser enviados no Authorization header, sendo do tipo bearer. O RefreshToken é enviado no método de atualização de tokens (signatureAccount/updateTokens). Para os restantes métodos, é enviado o AccessToken.

Sempre que o empresário pretenda efetuar uma assinatura, deve ser invocado o método credentials/authorize. Neste método devem ser enviada(s) a(s) hash(es) do(s) documento(s) a assinar. Para além disso, também de ser enviado, na mesma ordem, o(s) nome(s) do(s) documento(s) a assinar. O método devolve um Signature Activation Data (SAD) que terá de ser enviado no pedido de assinatura.

No método signatures/signHash são novamente enviada(s) a(s) hash(es) do(s) documento(s) a assinar assim como o SAD devolvido no passo anterior. O método devolve a(s) hash(es) assinada(s). Neste passo, o Software

de Faturação deve construir o documento assinado, juntando, ao documento original, a hash assinada do documento e os certificados obtidos no método credentials/info.

No caso do AccessToken se encontrar expirado, o SAFE devolve um erro HTTP 401 Unauthorized, com a mensagem de erro “The access or refresh token is expired or has been revoked”. Nestes casos, o Software de Faturação deve invocar o método SignatureAccount/updateTokens de modo a ser gerado um novo accessToken e um novo refreshToken. Estes novos tokens devem ser utilizados nas invocações futuras ao SAFE. No caso em que o empresário pretenda cancelar a conta de assinatura, deve ser invocado o método signatureAccount/cancelAccount. Mais detalhes destes fluxos e métodos podem ser consultados no manual de integração do SAFE.

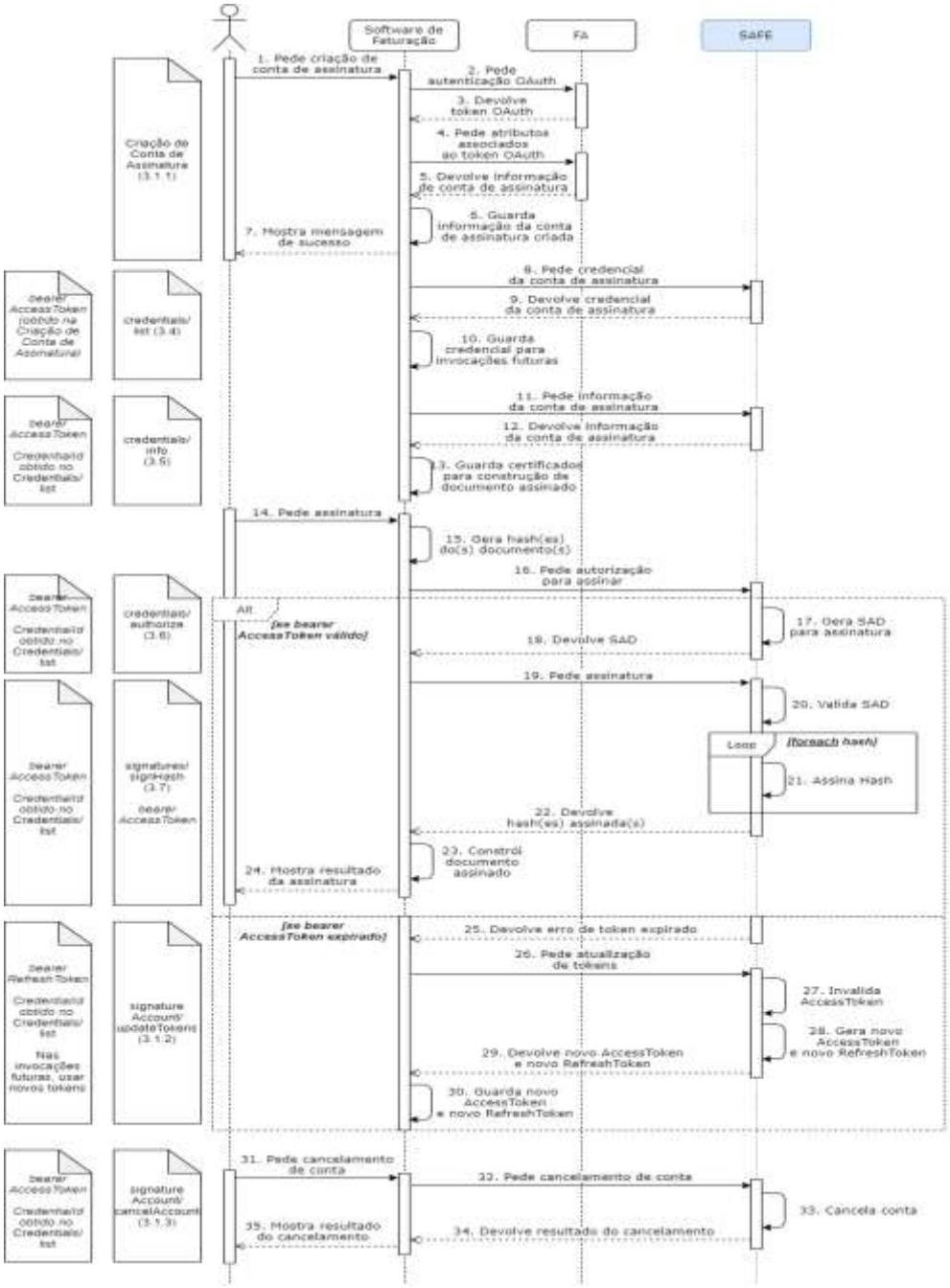


Figura 5. Fluxo típico

3. Âmbito dos Serviços

Nesta secção procede-se à descrição sumária das principais áreas de trabalho e atividades que se pretende que a equipa do cocontratante venha a desenvolver no âmbito deste projeto.

3.1 Objetivos e atividades no âmbito deste procedimento

3.1.1. Auditoria ao Prestador Qualificado de Serviços de Confiança AMA

1. Auditoria de acompanhamento a Serviços de confiança de certificados qualificados de assinaturas eletrónica, com serviço de aposição de assinatura eletrónica qualificada criada através de dispositivo de criação das assinaturas eletrónicas à distância (conforme indicado no considerando 52 do regulamento eIDAS). Esta auditoria tem como finalidade a manutenção da credenciação deste serviço, de acordo com o ponto 1 do artigo 20º do regulamento 910/2014 (eIDAS).

2. Auditoria para verificação de implementação de ações corretivas, caso a auditoria de acompanhamento seja considerada condicional face à verificação da implementação das ações corretivas.

Cláusula 15ª

Requisitos da equipa e Entidade a afetar aos serviços

1. A entidade deverá estar credenciada pelo IPAC, como organismo de avaliação de conformidade no âmbito do regulamento eIDAS, para a realização das auditorias alvo.
2. A equipa de auditoria deverá igualmente estar credenciada para a realização das auditorias alvo.

Cláusula 16ª

Planeamento

1. Os serviços suprarreferidos deverão ser iniciados após a celebração do contrato e integralmente concluídos num prazo de 4 semanas.
2. O cocontratante deve apresentar na sua proposta um calendário para o desenvolvimento dos serviços apresentados no ponto 3.1 da cláusula 14.ª, com indicação clara da alocação dos recursos e sua alocação às diferentes fases e entregáveis do projeto.
3. O planeamento apresentado pode vir a sofrer alterações em função de prioridades no decurso do projeto, ou em reunião de Kick-Off do projeto.

Cláusula 17ª

Entregáveis e documentação

1. O cocontratante entregará à AMA, conforme faseamento dos trabalhos, no mínimo, a seguinte documentação em suporte digital (.pdf e .odf):
    a) Relatório de auditoria e avaliação de conformidade;
    b) Revisão de Relatório de auditoria considerando eventuais ações corretivas.
2. A AMA poderá proceder à reprodução de todos os documentos referidos no número anterior (para os fins que assim o entender).

Cláusula 18ª

Mecanismos formais de acompanhamento

1. No âmbito da prestação de serviços objeto do presente procedimento o cocontratante deverá respeitar a orgânica indicada na sua proposta para a realização dos trabalhos e a coordenação conjunta do projeto com a AMA, incluindo os diversos níveis.
2. Deverá também assegurar os mecanismos propostos para efeitos de gestão e acompanhamento dos trabalhos do projeto, que inclui os instrumentos de controlo, periodicidade e forma como serão envolvidos no projeto, do ponto de vista do seu acompanhamento, bem como os vários níveis constituintes da orgânica definida, tendo em consideração os seguintes requisitos:

    a) Todos resultados produzidos pelo cocontratante no âmbito do presente fornecimento deverão ser alvo de aceitação por parte da AMA;

    b) A AMA terá um prazo de 2 semanas para se pronunciar em relação aos resultados apresentados pelo cocontratante.

    c) No caso da não-aceitação, por parte da AMA, dos resultados, deverá o cocontratante (num prazo inferior a 5 dias) proceder às alterações necessárias para nova análise da AMA (nos termos supra).

Cláusula 19ª

Gestor do Contrato

1. O gestor do contrato, com a função de acompanhar permanentemente a execução contratual, nos termos e para os efeitos previstos no artigo 290.º-A do CCP, será designado pela AMA no contrato.

2. O cocontrantante deverá indicar a pessoa na sua organização que será responsável pela execução do contrato, e que será o interlocutor com o gestor do contrato designado pela AMA, bem como a pessoa responsável pelo tratamento de dados pessoais.